Labor Automatisierungstechnik - User Manual

Thimo Langbehn

10. Dezember 2013

Inhaltsverzeichnis

1 Kerberos **2**
- 1.1 Voraussetzungen . . . 2
- 1.2 Programme . . . 2
- 1.3 Konfiguration . . . 2
  - 1.3.1 Windows XP . . . 3
  - 1.3.2 Windows 7 64Bit oder Vista 64Bit . . . 3
- 1.4 Verwendung . . . 3
  - 1.4.1 Leash für Windows . . . 4
  - 1.4.2 Passwort ändern . . . 4
- 1.5 Fehlerbehebung . . . 4

2 SVN **5**
- 2.1 Voraussetzungen . . . 5
- 2.2 Programme . . . 5
- 2.3 Konfiguration . . . 5
  - 2.3.1 Tortoise SVN . . . 5
  - 2.3.2 Eclipse . . . 5
- 2.4 Verwendung . . . 5
- 2.5 Test . . . 6
  - 2.5.1 Windows . . . 6
- 2.6 Migration von Alten Checkouts (Working Copy) . . . 6
  - 2.6.1 Windows . . . 6

3 Andrew File System (AFS) **6**
- 3.1 Voraussetzungen . . . 6
- 3.2 Programme . . . 6
- 3.3 Konfiguration . . . 7
  - 3.3.1 OpenAFS für Windows XP . . . 7
  - 3.3.2 OpenAFS auf Windows 7 64Bit oder Vista 64Bit . . . 7
- 3.4 Test . . . 8
- 3.5 Fehlerbehebung . . . 8

1 Kerberos

Um in den vollen Genuss der Möglichkeiten eines Kerberos-Systems (Single Sign On) zu kommen muss man eine Kerberos-Implementierung installieren. Die Implementierung besteht im wesentlichen aus einer Kerberos Bibliothek und einigen Programmen zur Ticket(cache) Verwaltung.

1.1 Voraussetzungen

- Die Namensauflösung für die Domäne **„beuth-hochschule.de“** muss funktionieren. Die korrekten Nameserver für die BHT sind:
  141.64.3.55 (dnsmaster.beuth-hochschule.de)
  141.64.3.40 (dnsslave.beuth-hochschule.de)
  Der DNS-Server mit der IP 141.64.224.200 ist veraltet und soll nicht mehr verwendet werden. Er wird bei Kerberos zu Problemen führen.
- Der Host **„lat30.beuth-hochschule.de“** muss erreichbar sein (**UDP Port 88**).

1.2 Programme

Windows XP Hierfür gibt es das MIT Kerberos for Windows (KfW). Es existieren zwei Versionen, eine ältere, Leash, und eine neuere, der Network Identity Manager (NIM). Zweiterer integriert das AFS besser und ermöglicht es auch mehrere TGTs zu verwalten. Der NIM wird empfohlen.

- Leash 32Bit: `http://mit.edu/kerberos/dist/kfw/2.6/kfw-2.6.5/MITKerberosForWindows-2.6.5.msi`
- NIM 32Bit: `http://mit.edu/kerberos/dist/kfw/3.2/kfw-3.2.2/kfw-3-2-2.msi`

Windows 7 64Bit oder Vista 64Bit Bei diesen Systemen kann man eine 32-Bit Variante installieren (siehe oben) ,eine 64Bit Variante oder beides. Wichtig ist, dass für alle Programme die Kerberos nutzen sollen ebenfalls die entsprechende Variante (32Bit bzw. 64Bit) installiert wird.

Hinweis: Einige Programmen sind noch nicht mit 64-Bit Kerberos nutzbar, dies betrifft insbesondere SVN (TortoiseSVN) und SSH (PuTTY).

- NIM 64Bit: `http://www.secure-endpoints.com/binaries/mit-kfw-3-2-2/kfw-amd64-3-2-2.msi`
- KCA-Plugin 64Bit: `http://www.secure-endpoints.com/binaries/kcaplugin-amd64-2_2_0_2.msi`

1.3 Konfiguration

Die Bibliothek muss über eine Konfigurationsdatei eine Liste von sogenannten Realm Spezifikationen erhalten, um einer DNS Adresse einen Realm, und diesem einen KDC-Server zuzuordnen. Sie muss wie folgt abgeändert werden:

```
[libdefaults]
```

```
  default_realm = LAT.BEUTH-HOCHSCHULE.DE
  dns_lookup_kdc = true
[realms]
  LAT.BEUTH-HOCHSCHULE.DE = {
    admin_server = lat30.beuth-hochschule.de
    kdc = lat30.beuth-hochschule.de
  }
[domain_realm]
  beuth-hochschule.de = LAT.BEUTH-HOCHSCHULE.DE
  .beuth-hochschule.de = LAT.BEUTH-HOCHSCHULE.DE
[logging]
```

Die restlichen Realm-Beschreibungen (in der Sektion **[Realms]**) können bestehen bleiben.

Diese Datei ist insofern nicht sicherheitskritisch, als dass sie problemlos gelesen werden darf. Schreibzugriff sollte allerdings nur einem Administrator gestattet sein. Ansonsten könnte durch Manipulation der **kdc** und **admin_server** Adresse eine Spoofing-Attake eingeleitet werden.

1.3.1 Windows XP

Unter Windows heißt diese Datei **„krb5.ini“**, und befindet sich standardmäßig im Windows-Verzeichnis.

Nach den oben beschriebenen Anpassung muss unter Windows Leash bzw. der NIM neu gestartet werden. Um andere Anwendungen mit Kerberos zusammenzubringen, muss noch die **„krb5_32.dll“** aus dem Kerberos Programmverzeichnis in das **Windows/System32** Verzeichnis kopiert werden. Nach diesen Einstellungen muss Windows **zwei mal** neu gestartet werden.

1.3.2 Windows 7 64Bit oder Vista 64Bit

Unter Windows heißt diese Datei **„krb5.ini“**, und befindet sich standardmäßig im Windows-Verzeichnis. Um sie zu ändern muss man entweder als Administrator angemeldet sein oder aber dem angemeldeten User Schreibrechte auf die Datei geben. In dem zweiten Falle sollte nicht vergessen werden die Schreibrechte nach der Anpassung wieder zu entfernen.

Nach den oben beschriebenen Anpassung muss unter Windows Leash bzw. der NIM neu gestartet werden. Um andere Anwendungen mit Kerberos zusammenzubringen, muss noch die **„krb5_64.dll“** aus dem Kerberos Programmverzeichnis in das **Windows/System32** Verzeichnis kopiert werden. Nach diesen Einstellungen muss Windows **zwei mal** neu gestartet werden.

1.4 Verwendung

Voraussetzungen für die Verwendung von Kerberos sind die oben beschriebenen Einstellungen, eine bestehende Netzwerkverbindung (Internet) und Verfübarkeit des korrekten DNS-Servers. Weiterhin muss die Uhrzeit des Rechners korrekt eingestellt sein.

1.4.1 Leash für Windows

Zeitsynchronisation In Windows kann die Zeit Synchronisation bequem per **Action -> Synchronize Time** in Leash erfolgen.

Einloggen Nach dem Start von Leash kann in diesem mittels **Action -> Get Ticket(s)** oder CTRL+T kann nun ein Ticket Granting Ticket (TGT) angefordert werden. Name und Passwort müssen die de eigenen Accounts sein, der Realm muss dabei auf **LAT.BEUTH-HOCHSCHULE.DE** stehen. Wenn die Aktion erfolgreich war, so befindet sich nun in dem unteren Bereich des Fensters ein grünes Symbol mit dem Eintrag **user@LAT.BEUTH-HOCHSCHULE.DE**.

Passwort ändern 1.4.2 Passwort ändern

Das Passwort kann geändert werden, indem man sich per ssh auf z.B. per ssh auf z.B. **lat.beuth-hochschule.de** einwählt, und dort das Programm **$> kpasswd** aufruft.

1.5 Fehlerbehebung

1. Synchronisiere die Zeit mit einem Internet-Zeitserver. Sollte dies mit einer Fehlermeldung abbrechen, oder die Zeit nicht korrekt synchronisiert werden, so kann eine Ursache dafür in einer dazwischenliegenden Firewall liegen. In diesem Fall kann die Zeit auch manuell gestellt werden. Sie muss nur innerhalb einer Toleranz von 5 Minuten korrekt sein.

2. führe ein **$> ping lat30.beuth-hochschule.de** aus, dabei sollte der Name in die korrekte IP (**141.64.75.95**) aufgelößt werden.

   Funktioniert dieser Test nicht, dann arbeitet die DNS-Auflöung nicht richtig. Dass kann an einem fehlerhaften Nameserver liegen, oder auch an überchreibenden Einstellungen des Clients bzw. alten Werten in dessen Puffer.

   Eine andere IP (nicht 141.64.75.95) wird angezeigt Irgendein Nameserver oder Cache liefert die falschen Werte zurück. Überprüfe die hosts Datei. Diese findet sich unter Windows in **C:\Windows\System32\drivers\etc\hosts**, und unter Linux in **/etc/hosts**. Suche nach Einträgen der Domain **„beuth-hochschule.de“**. Diese sollten entfernt werden, sie sind nur nötig wenn der Nameserver keine korrekten Ergebnisse liefert.

   Es wird gar keine IP angezeigt Die Domäne wird von dem lokalen Nameserver nicht richtig aufgelößt. Trage die folgenden Einträge in die oben gennante hosts Datei ein:

   ```
   141.64.75.95  lat30.beuth-hochschule.de
   ```

3. Überprüfe deine Firewall, ob sie ausgehende Verbindungen zum **UDP Port 88** von **141.64.75.95** zulässt. Ein Test in einer weniger restriktiven Umgebung kann Unklarheiten bezüglich anderer, dazwischen liegender Umgebungen beseitigen).

2 SVN

Auf dem Server können eine beliebige Anzahl von SVN Repositories betrieben werden, sei es für den ausschließlich eigenen Gebrauch, oder für eine Gruppe.

Zugriff auf die SVN Repositories erfolgt direkt über das svn Protokoll:

2.1 Voraussetzungen

- Kerberos muss eingerichtet sein.
- **lat30.beuth-hochschule.de** muss erreichbar sein.

2.2 Programme

Windows XP hat den TortoiseSVN Client zur Verfügung, hier muss mindestends die Version 1.5 verwendet werden.
`http://downloads.sf.net/tortoisesvn/` Weiterhin muss die saslGSSAPI.dll installiert werden. Hierbei handelt es sich um ein GSSAPI (Kerberos5) Plugin für eine Authentifizierungsschicht (Cyrus SASL)
`http://lat.beuth-hochschule.de/downloads/saslGSSAPI.dll`(32-Bit)

Windows 7 64Bit oder Vista 64Bit Hierfür existiert zwar bereits eine TortoiseSVN 64Bit Version:
`http://downloads.sf.net/tortoisesvn/`
Allerdings fehlt derzeit (März 2010) noch das die benötigte saslGSSAPI.dll in einer 64Bit Version. Somit kann SVN als 64Bit Lösung derzeit nicht mit Kerberos unter Windows verwendet werden. Für die 32-Bit Lösung muss dann auch Kerberos in 32-Bit installiert sein.

2.3 Konfiguration

2.3.1 Tortoise SVN

Die Heruntergeladenen **saslGSSAPI.dll** muss in das bin Verzeichnis des installierten TortoiseSVN kopiert werden (normalerweise **C:\Programme\TortoiseSVN\bin**).

Danach muss der Rechner einmal neu gestartet werden.

2.3.2 Eclipse

Um SVN aus Eclipse heraus nutzen zu können, beispielsweise mit Subclipse (`http://subclipse.tigris.org/`), muss die Kerberos-Authentifizierung für diese Plugins nachgerüstet bzw. aktiviert werden. Für Linux und Windows hält das MIT eine Anleitung vor: `https://wikis.mit.edu/confluence/display/ISTMAP/Integrating+MyEclipse+and+Subversion`. Während der erste Absatz MyEclipse-spezifisch ist, kann der Rest auch bei anderen Eclipse-Integrationen Anwendung finden.

2.4 Verwendung

Vor dem Zugriff auf Kerberos-basierte SVN Repositories muss ein Ticket angefordert werden. Je Nach Anmeldeclient wird, sollte dieses zum Zugriffszeitpunkt

nicht vorhanden sein, die Eingabe der User-Credentials gefordert. Dies ist jeduch nur einmalsig im Gültigkeitszeitraum des Tickets notwendig.

Wenn ein Ticket vorhanden ist, können vorhandenen Repositories unter der URL **svn://lat30.beuth-hochschule.de/REPOSITORY** angesprochen werden. **REPOSITORY** muss hierbei natürlich durch einen gültigen namen ersetzt werden.

2.5 Test

Als Beispiel und zum Experimentieren kann das **sandbox** Repository verwendet werden, die dazugehörige URL lautet **svn://lat30.beuth-hochschule.de/sandbox**.

Dazu bedarf es folgender Schritte:

2.5.1 Windows

Mit der Rechten Maustaste auf ein neu angelegtes, leeres Verzeichnis (oder auf eine freie Fläche in einem geöffneten Ordner) klicken, und SVNCheckout aus dem dann aufklappenden Kontextmenü auswählen.

In der oberen Zeile des Checkout-Dialogs nun die gewünschte URL angeben und mit OK bestätigen.

Der checkout sollte erfolgreich durchgeführt werden können, in dem ausgewählten (oder neu erstellten) Ordner sollten nun einige Dateien zu finden sein.

2.6 Migration von Alten Checkouts (Working Copy)

2.6.1 Windows

Mit der Rechten Maustaste auf das Wurzelverzeichniss des Checkouts klicken. In dem daraufhin erscheinenden Kontextmenü **relocate** auswählen.

Die neue URL kann durch Ersetzen des ersten Teils (bis zum Repository-Namen mit **svn://lat30.beuth-hochschule.de/sandbox** gebildet werden. Die so gebildete URL eintragen (z.B. *svn://lat30.beuth-hochschule.de/sandbox*) und bestätigen.

3 Andrew File System (AFS)

3.1 Voraussetzungen

- Kerberos muss eingerichtet sein.
- Ein entsprechender Account muss eingerichtet sein.
- **lat30.beuth-hochschule.de** muss erreichbar sein.

3.2 Programme

Windows XP user müssen sich einen der OpenAFS (`http://www.openafs.org/`) installer herunterladen.
`http://dl.openafs.org/dl/openafs/1.5.54/winxp/OpenAFSforWindows-1-5-54.exe` (32-Bit)

Windows 7 64Bit oder Vista 64Bit können die 64Bit Variante verwenden, so sie ein 64Bit Kerberos installiert haben.
`http://dl.openafs.org/dl/openafs/1.5.54/winxp/openafs-en_US-64bit-1-5-54.msi` (64-Bit)

3.3 Konfiguration

3.3.1 OpenAFS für Windows XP

OpenAFS liegt für Windows in zwei Varianten zur Installation vor. Einmal als .exe für die manuelle Installation und einmal als .msi für eine gemanagete Installation mit Hilfe eines Wizards. Es wird empfohlen, die manuelle Installation zu wählen. Diese wird hier detailiert beschrieben. Für die Installation und Konfiguration muss der Nutzer Admin-Rechte besitzen.

Nachdem den Lizenzbedingungen zugestimmt wurde, kann zwischen verschiedenen Arten der Installation gewählt werden. Hier sollte die Wahl auf *AFS Client* fallen. Nachdem ein Installationsverzeichnis gewählt wurde wird die Frage nach der *CellServDB* gestellt. Hier sollte die Option „download from“ gewählt und folgende Adresse eingetragen werden: `http://lat.beuth-hochschule.de/downloads/CellServDB`

Im nächsten Schritt wird nach dem Zellenname der AFS Zelle gefragt. Der Name lautet *lat.beuth-hochschule.de*. Die restlichen Optionen können so gelassen werden, wie sie vorgegeben sind. Nach der Installation muss das System neu gestartet werden.

Nach dem Neustart versucht AFS eventuell ein Ticket zu bekommen. Das sollte erst einmal abgebrochen werden, da noch einige Konfigurationen fehlen.

Wenn als Kerberos Client der Network Identity Manager (NIM) anstelle von Leash verwendet wird, sollte dort unter Options→AFS die Option „Prevent AFSCreds.exe from starting automatically when you log in to Windows.“ aktiviert werden.

Danach sollte das *OpenAFS Control Panel* geöffnet und dort sichergestellt werden, dass die Option „AFS-Token beim Anmelden bei Windows erhalten“ deaktiviert ist.

Zusätzlich können in dem Tab *Laufwerkbuchstaben* beliebige Laufwerksbuchstaben Pfaden im AFS zugeordnet werden. Der Grundpfad ist dabei immer \afs\lat.beuth-hochschule.de. Weitere Verzichnisse können nach belieben angehangen werden. Um zum Beispiel das eigene Home-Verzeichnis an den Buchstaben „Z“ zu binden, muss nur der Buchstabe ausgewählt werden und er Pfad „\afs\lat.beuth-hochschule.de\user\USER“ benutzt werden, wobei USER natürlich durch den eigenen Username ersetzt werden muss.

3.3.2 OpenAFS auf Windows 7 64Bit oder Vista 64Bit

Die Installation kann genau so vorgenommen werden wie bei Windows XP, jedoch muss die richtige Version (32Bit oder 64Bit) verwendet werden.

3.4 Test

3.5 Fehlerbehebung

- Die Systemzeit des eigenen Rechners muss korrekt sein. Eine Differenz von mehr als drei Minuten wird das Anfordern von Kerberos-Tickets oder AFS-Tokens verhindern.
- Das KDC und der AFS Fileserver (lat30.beuth-hochschule.de) müssen erreichbar sein.